Możliwość dofinansowania

Cyberbezpieczeństwo i RODO w ochronie zdrowia

Numer usługi 2025/05/14/169989/2744470

2 250,00 PLN brutto
2 250,00 PLN netto
112,50 PLN brutto/h
112,50 PLN netto/h

WELLNESS PROGRESSIVE GROUP POLSKA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

73 oceny

Toruń / stacjonarna
Usługa szkoleniowa
20 h
06.09.2025 do 07.09.2025

Informacje podstawowe

Kategoria	Zdrowie i medycyna / Medycyna
Grupa docelowa usługi	Fizjoterapeuci
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	05-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	20
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa przygotowuje do identyfikowania zagrożeń cybernetycznych, zarządzania ryzykiem oraz wdrażania skutecznych środków ochrony danych osobowych zgodnie z RODO i przepisami krajowymi. Szkolenie pozwala uczestnikom zdobyć praktyczne kompetencje w zakresie zabezpieczania systemów teleinformatycznych, reagowania na incydenty bezpieczeństwa oraz prawidłowego przetwarzania danych osobowych w podmiotach ochrony zdrowia

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje podstawowe zagrożenia cybernetyczne i typowe scenariusze ataków	Omawia przykłady zagrożeń i sposoby działania cyberprzestępców	Obserwacja w warunkach rzeczywistych
Wskazuje sposoby reagowania na incydenty bezpieczeństwa	Opisuje procedurę postępowania i zgłaszania incydentu	Obserwacja w warunkach rzeczywistych
Efekty uczenia się Kryteria weryfikacji Metody walidacji Identyfikuje podstawowe zagrożenia cybernetyczne i typowe scenariusze ataków Omawia przykłady zagrożeń i sposoby działania cyberprzestępców Studium przypadku, analiza scenariuszy Określa zasady zarządzania ryzykiem w kontekście cyberbezpieczeństwa Tworzy przykładowy schemat oceny ryzyka i doboru zabezpieczeń Praca zespołowa, ćwiczenia praktyczne Interpretuje wymagania KRI i przepisów dotyczących bezpieczeństwa informacji Wskazuje zależności między dokumentacją, audytem a bezpieczeństwem systemów Test wiedzy, analiza materiałów prawnych Wskazuje sposoby reagowania na incydenty bezpieczeństwa Opisuje procedurę postępowania i zgłaszania incydentu Ćwiczenie symulacyjne, arkusz sytuacyjny Rozpoznaje podstawowe pojęcia związane z RODO i ochroną danych osobowych	Poprawnie stosuje pojęcia w kontekście konkretnych przypadków	Obserwacja w warunkach rzeczywistych
Analizuje konsekwencje prawne naruszeń ochrony danych osobowych	Opisuje skutki naruszeń i obowiązki wynikające z przepisów	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

DZIEŃ I:

–**Wprowadzenie do cyberbezpieczeństwa**– Podstawowe pojęcia i definicje (zagrożenia, podatności, ryzyko, incydenty)

Rodzaje zagrożeń cybernetycznych (malware, phishing, ataki DDoS, socjotechnika)

Aktualne trendy w cyberprzestępczości Krajowe Ramy Interoperacyjności (KRI) – podstawy prawne i zakres

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne

Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności

Minimalne wymagania dla rejestrów publicznych i wymiany informacji

Minimalne wymagania dla systemów teleinformatycznych

Cyberbezpieczeństwo w KRI

Zarządzanie bezpieczeństwem informacji w kontekście KRI

Wymagania KRI dotyczące bezpieczeństwa systemów teleinformatycznych

Polityka bezpieczeństwa informacji a KRI

Audyt bezpieczeństwa a KRI

–**Zarządzanie ryzykiem w cyberbezpieczeństwie**– Identyfikacja i analiza ryzyka

Metody oceny ryzyka

Wybór i wdrożenie zabezpieczeń

Monitorowanie i przegląd ryzyka

Praktyczne aspekty cyberbezpieczeństwa Bezpieczne hasła i uwierzytelnianie

Ochrona przed phishingiem i socjotechniką

Bezpieczne korzystanie z poczty elektronicznej i internetu

Ochrona danych osobowych (RODO) w kontekście cyberbezpieczeństwa

–**Bezpieczeństwo systemów i aplikacji-** Zabezpieczanie systemów operacyjnych

Bezpieczeństwo aplikacji i baz danych

Aktualizacje oprogramowania

Kopie zapasowe i plany odzyskiwania danych

Reagowanie na incydenty bezpieczeństwa (30 min)

Procedury postępowania w przypadku incydentu

Zgłaszanie incydentów

Analiza i likwidacja skutków incydentów

Działania prewencyjne

–**Warsztaty praktyczne**– Warsztaty praktyczne

Analiza przykładowych scenariuszy ataków

Dyskusja i wymiana doświadczeń

DZIEŃ II

— **Dane Osobowe** – podstawowe pojęcia: Ochrona danychosobowych w polskim prawodawstwie: Zasady przetwarzania danych osobowych: Formy przetwarzania danych osobowych- Wprowadzenie do podstawowych pojęć związanych z danymi osobowymi, takich jak dane osoboweprzetwarzanie, administrator danych, podmiot przetwarzający, dane wrażliwe. Wyjaśnienie terminologii stosowanej w przepisach RODO. Omówienie najważniejszych przepisów dotyczących ochrony danych osobowych w polskim systemie prawnym, w tym związków z przepisami unijnymi, głównie RODO, oraz implementacji przepisów na poziomie krajowym. Przedstawienie fundamentalnych zasad przetwarzania danych osobowych zgodnych z RODO, takich jak legalność, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość oraz integralność i poufność. Omówienie różnych form przetwarzania danych, takich jak zbieranie, przechowywanie, przekazywanie, anonimizacja, archiwizacja, usuwanie i niszczenie danych. Analiza typowych działań przetwarzania w kontekście projektów.

–**Obszar przetwarzania danych:** Dostęp do danych osobowych: Zasady zabezpieczania danych osobowych: Obowiązki osób przetwarzających dane osobowe:-Wyjaśnienie, co oznacza obszar przetwarzania danych, omówienie zakresu geograficznego, a także granic przetwarzania danych w ramach UE i poza nią, w tym przepływu danych transgranicznego oraz zasad ochrony danych w przypadku outsourcingu. Przedstawienie zasad dostępu do danych osobowych przez osoby upoważnione. Procedury przyznawania uprawnień i obowiązki dotyczące ich monitorowania orazwycofywania, jeśli dostęp nie jest już konieczny. Omówienie technicznych i organizacyjnych środków bezpieczeństwa wymaganych do skutecznego zabezpieczenia danych osobowych, takich jak szyfrowanie, kontrola dostępu, zabezpieczenia fizyczne i elektroniczne, a także audyty i analiza ryzyka. Przedstawienie odpowiedzialności i obowiązków osób, które mają dostęp do danych osobowych, w tym przestrzegania polityk bezpieczeństwa, procedur, szkoleń oraz obowiązku zgłaszania incydentów.

–**Prawa osoby, której dane dotyczą**: Odpowiedzialność prawna osoby przetwarzającej dane osobowe: Przepisy wewnętrzne PW o ochronie danych osobowych:-Omówienie praw przysługujących osobom, których dane są przetwarzane, w tym prawa dostępu do danych, ich sprostowania, usunięcia („prawo do bycia zapomnianym"), ograniczenia przetwarzania, przenoszenia oraz prawa do sprzeciwu wobec przetwarzania danych. Analiza konsekwencji prawnych i finansowych wynikających z naruszenia przepisów RODO, w tym kar administracyjnych, odpowiedzialności cywilnej i karnej, a także sankcji związanych z nieprzestrzeganiem zasad ochrony danych. Omówienie wewnętrznych regulacji uczelni (PW) dotyczących ochrony danych, polityk i procedur obowiązujących pracowników oraz studentów, w tym wymagań dotyczących bezpieczeństwa i zarządzania danymi.

–**Pytania/dyskusja**:-Sesja pytań i odpowiedzi oraz dyskusja podsumowująca, umożliwiająca wyjaśnienie ewentualnych wątpliwości i omówienie przypadków praktycznych, z którymi uczestnicy mogą mieć do czynienia w kontekście ochrony danych osobowych.

Harmonogram

Liczba przedmiotów/zajęć: 13

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Wprowadzenie do cyberbezpieczeństwa – pojęcia, zagrożenia, trendy	-	06-09-2025	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 13 Krajowe Ramy Interoperacyjności (KRI) – podstawy prawne i wymogi	-	06-09-2025	10:30	12:00	01:30
3 z 13 Zarządzanie ryzykiem – identyfikacja, metody oceny, wdrażanie zabezpieczeń	-	06-09-2025	12:00	13:30	01:30
4 z 13 Przerwa	-	06-09-2025	13:30	14:00	00:30
5 z 13 Praktyczne aspekty cyberbezpieczeństwa + reagowanie na incydenty	-	06-09-2025	14:00	15:30	01:30
6 z 13 RODO: pojęcia, podstawy prawne, zasady przetwarzania danych osobowych. Obszary przetwarzania danych - cz.1	-	06-09-2025	15:30	18:00	02:30
7 z 13 Obszary przetwarzania danych, dostęp, zabezpieczenia, obowiązki	-	07-09-2025	08:00	09:30	01:30
8 z 13 Prawa osób, odpowiedzialność, dokumentacja i wewnętrzne procedury	-	07-09-2025	09:30	11:00	01:30
9 z 13 Przerwa	-	07-09-2025	11:00	11:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 13 Zarządzanie dostępem i uprawnieniami w systemach medycznych	-	07-09-2025	11:15	12:30	01:15
11 z 13 Bezpieczeństwo urządzeń mobilnych i pracy zdalnej	-	07-09-2025	12:30	14:00	01:30
12 z 13 Podsumowanie	-	07-09-2025	14:00	14:30	00:30
13 z 13 Walidacja	Mariusz Kończak	07-09-2025	14:30	14:45	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 250,00 PLN
Koszt przypadający na 1 uczestnika netto	2 250,00 PLN
Koszt osobogodziny brutto	112,50 PLN
Koszt osobogodziny netto	112,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Mariusz Kończak

Biegły sądowy w dziedzinie ochrony danych osobowych i informacji niejawnych w systemach informatycznych przy Sądzie Okręgowym w Poznaniu

Pełnomocnik ds. ochrony informacji niejawnych

Inspektor Ochrony Danych Osobowych

Auditor wewnętrzny ISO 27001

Doświadczony trener szkoleń biznesowych. Szkolenia prowadzi od kilkunastu lat.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na początku kursu uczestnicy otrzymują skrypt obejmujący materiał dydaktyczny przygotowany dla danego szkolenia.

Warunki uczestnictwa

Warunkiem uczestnictwa w kursie jest :

1. Posiadanie ważnego numeru ID wsparcia

2. Zapisanie się na wybraną usługę przez stronę www.well.edu.pl (z zaznaczeniem opcji: **Dofinansowanie BUR**)

Uprzejmie przypominamy, iż zgłoszenie na kurs przez BUR nie stanowi potwierdzenia udziału w kursie. **Obligatoryjny jest kontakt z Organizatorem w celu potwierdzenia wolnych miejsc oraz wykonanie czynności opisanych w pkt.2.**

3. W szkoleniu mogą wziąć udział osoby wskazane w sekcji "Grupa docelowa usługi"- w przypadku wątpliwości związanych z uprawnieniami dotyczącymi udziału w szkoleniach, prosimy o kontakt e-mailowy lub telefoniczny.

Informacje dodatkowe

Cena kursu nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności Organizator nie pokrywa oraz nie dokonuje zwrotu kosztów związanych z dojazdem uczestnika na usługę, jego zakwaterowaniem oraz wyżywieniem.

W liczbę godzin dydaktycznych kursu **nie są** wliczone przerwy.

Szkolenie jest zwolnione z podatku VAT na podstawie art. 43 ust. 1 punkt 26 podpunkt a ustawa o VAT lub w przypadku kursów dofinansowanych ze środków publicznych w min. 70% zwolnione z podatku VAT na podstawie art. 43 ust. 1 punkt 29 c.

W zależności od wymogów Operatorów i kwot dofinansowań, mogą pojawić się dodatkowe dopłaty do kursu.

Krótkie przerwy realizowane w czasie trwania kursu dostosowane są do tempa pracy uczestników podczas szkolenia. **Godziny przerw są podane orientacyjnie- w zależności od dynamiki i tempa grupy- mogą ulec zmianie.**

Adres

ul. Biała 2
87-100 Toruń
woj. kujawsko-pomorskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Jakub Ślaga

E-mail dofinansowania@well.edu.pl

Telefon (+48) 718 808 250